LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA, DOCUMENTO CONPES 3701

Fula Perilla, Pedro Antonio
pedrofula@gmail.com
Universidad Piloto de Colombia

Abstract— This is an analysis about cyber-attacks as one of the principal risks of global society those faces today, and initiatives generated to safeguard the privacy use, integrity and availability of information on public and private entities of the nation.

Resumen— Análisis sobre los ataques cibernéticos como uno de los principales riesgos a los que se enfrenta la sociedad globalizada de hoy, y las iniciativas generadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información en entidades publicas como privadas de la nación.

Índice de Términos— Ataques cibernéticos, ciberseguridad, ciberdefensa, confidencialidad, documento CONPES, disponibilidad, integridad.

I. INTRODUCCIÓN

La seguridad informática es un tema que atañe a la sociedad globalizada de hoy, por tanto, los gobiernos y entidades públicas y privadas de orden nacional e internacional, se han dado a la tarea de desarrollar acciones que garanticen la protección de los datos que circulan en la red. Con el desarrollo de Internet como una infraestructura global para los negocios, y como una nueva herramienta para la política, espionaje y las actividades militares, la ciberseguridad se ha convertido en tema central de la seguridad nacional e internacional.

En Colombia, una de estas iniciativas es el documento CONPES 3701, del consejo nacional de política económica y social, que establece los lineamientos para ciberseguridad y ciberdefensa, "orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país", administrado por tres grandes integrantes:

• Centro Cibernético Policial (CCP): "El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos".

• Comando Conjunto Cibernético (CCOC): Unidad Militar encargado de responder a los ataques cibernéticos contra los activos militares de la nación.

• colCERT: "Está conformando por un equipo de personas dedicadas a la gestión de incidente con el objetivo de mitigar el riesgo y dar respuesta a incidentes de tipo cibernético".

Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema" [1].

Todos los días se pueden encontrar artículos que cuentan sobre cómo una empresa ha sido víctima de delitos informáticos, y una de las causas es la falta de una adecuado plan de se seguridad; así mismo, el déficit de profesionales en el tema de ciberseguridad sigue siendo una vulnerabilidad crítica para las entidades y países, la educación y las políticas convencionales no pueden satisfacer la demanda. Se necesitan nuevas soluciones para construir un entorno necesario en ciberseguridad.

II. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

La posibilidad de acceso a Internet ha crecido en 354% entre 2005 y el 2009, como lo señala en documento CONPES, obligando esta situación a asumir retos de seguridad en medios electrónicos, puesto que a mayor acceso de usuarios a la red, mayor riesgo de ataque cibernético. Por ello, es necesario el "compromiso del gobierno nacional para garantizar la seguridad de la información" [1] que involucre al mismo tiempo a otras entidades públicas, además de la implementación de una política Nacional de ciberseguridad y ciberdefensa, que permita salvaguardar la confidencialidad, integridad y disponibilidad de la información a nivel nacional, regional y personal, tanto del orden público como privado.

III. ANTECEDENTES

El documento CONPES expone una serie de antecedentes de ataques cibernéticos que dan cuenta de la importancia de asumir acciones en torno a esta problemática. Entre los más representativos, se encuentra el ataque cibernético a Estonia en el año 2007, que requirió la intervención de la OTAN, ya que dicha institución se vio obligada a crear el centro de excelencia para la cooperación en ciberdefensa. Con base en esta situación y su impacto generado, "es considerado el mayor ataque cibernético de la historia" [1]. La casa blanca en Estados Unidos, el departamento de defensa, La administración federal de aviación y la comisión federal de comercio, también han sido blancos de ataques cibernéticos. Otro suceso que cabe mencionar se presentó en la guardia civil española en 2010 "cuando desmanteló a una de las mayores redes de computadores ´zombies´, conocida con el nombre de, botnet mariposa, compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo" [1], como se muestra en la siguiente tabla.

TABLA I
PAÍSES LATINOAMERICANOS MÁS AFECTADOS POR UNA RED DE ZOMBIES EN MARZO 2010.

No.	PAIS	%
1	INDIA	19.14
2	MÉXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	COLOMBIA	4.94
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55
11	PERÚ	2.42
12	IRÁN	2.07
13	ARABIA SAUDÍ	1.85
14	CHILE	1.74
15	KAZAKHSTAN	1.38
16	EMIRATOS ARABES	1.15
17	MARRUECOS	1.13
18	ARGENTINA	1.10
19	ESTADOS UNIDOS	1.05

Fuente: Documento CONPES 3701 [1]

Un estudio realizado por la firma symantec, especialista en soluciones de seguridad, determinó "que los ataques cibernéticos de los que han sido víctimas las empresas del sector privado le ha costado a cada una de ellas, un promedio de dos millones de dólares al año" [7].

El 42% de las entidades que se vieron involucradas determinó a la seguridad informática como su principal objetivo, teniendo en cuenta que el 75% de ellas sufrió algún tipo de incidente en su componente de seguridad durante los 12 meses anteriores a la realización del estudio. Argumentado que la "escasez de personal, las nuevas iniciativas de tecnologías de la información y los problemas de cumplimiento de las normas de tecnologías de la información son factores críticos para la seguridad" [7].

Colombia no ha sido la excepción de este tipo de ataques; para el año 2011 "el grupo "hacktivista" autodenominado anonymous, atacó los portales web de la presidencia de la república, del senado y de los ministerios del interior, de justicia, cultura y defensa, dejando fuera de servicio sus páginas web por varias horas" [1] esto sin tener en cuenta las múltiples denuncias de ciudadanos, que han sido víctimas de diversas formas de delitos informáticos reportados por la policía nacional.

IV. MARCO NORMATIVO

Actualmente se está viviendo un período decisivo en la ciberseguridad, noticias de informes diarios incidentes cibernéticos a gran escala son cada vez más objeto de escenarios políticos. Uno de los mayores temores de los ataques cibernéticos es paralizar las infraestructuras críticas generando caos. Sin embargo, para mantener el ritmo de los que tratan de aprovechar las vulnerabilidades digitales, aún queda mucho por hacer. En la mayoría de países, las personas tienen que tomar nota de cómo usan Internet y garantizar que tienen en cuenta todas las precauciones para proteger sus datos y dispositivos de uso diario. El Internet es un bien compartido y la ciberseguridad es una responsabilidad compartida, es decir, las personas tienen que practicar hábitos seguros en línea. Las TIC es probable que continúe creciendo constantemente. De acuerdo con ello, los gobiernos deben tomar medidas apropiadas para proteger y asegurar sus infraestructuras críticas para promover la planificación y la legislación de ciberseguridad.

En cuanto a la legislación que aborda el tema, Colombia desde el año 2007 hasta el 2009, a través de iniciativas legales como leyes, resoluciones, circulares e iniciativas que han buscado prevenir, proteger y contrarrestar los ataques cibernéticos, como la circular 052 de 2007 de la superintendencia financiera de Colombia, que establece "los requerimientos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios" [1]. Del mismo modo, la adopción de convenios y resoluciones de ámbito internacional conducentes al mismo fin, como lo es la resolución 64-25 que hace

referencias a los "avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad nacional e internacional" [1], promulgada en la asamblea general de las naciones unidas en el año 2009.

En la siguiente tabla se puede observar de forma cronológica la normativa Nacional relacionada con seguridad de la información:

TABLA II
NORMATIVIDAD NACIONAL

LEY / RESOLUCION CIRCULAR	TEMA
Ley 527 de 1999 - COMERCIO ELECTRÓNICO	"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
Ley 962 de 2005	"Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los tramites por parte de los administrados".
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	"Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios".
Ley 1266 de 2008	"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
Ley 1273 de 2009	"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
Ley 1341 de 2009	"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la agencia nacional del espectro y se dictan otras disposiciones".
Documento CONPES 3701 de 2011	"Lineamientos de política para ciberseguridad y ciberdefensa".
Ley 1581 de 2012	"Por la cual se dictan disposiciones generales para la protección de datos personales".

Fuente: Documento CONPES 3701 [1]

Pese al interés del gobierno Colombiano por garantizar la seguridad de la información que circula en la red, y evitar los ataques cibernéticos, según el documento CONPES, son evidentes los siguientes ejes que acrecientan el problema: las iniciativas y operaciones en ciberseguridad y ciberdefensa no están coordinadas adecuadamente; debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa y la insuficiente regulación para la protección de la información y de los datos. De otro lado, el documento CONPES también señala un plan de acción descrito en veintidós acciones concretas, conducentes al alcance del objetivo central "fortalecer las capacidades del estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio; junto con sus tres objetivos específicos:

1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional.

2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa.

3) Fortalecer el cuerpo normativo y de cumplimiento en la materia. [1].

Es de aclarar que algunos países se han puesto en la tarea de realizar acciones en materia de ciberseguridad y ciberdefensa según lo menciona el documento CONPES en la siguiente tabla:

TABLA III
ACCION TOMADA EN MATERIA DE CIBERSEGURIDAD Y CIBERDEFENSA

PAÍS	ACCIÓN TOMADA POR EL GOBIERNO
ALEMANIA	En febrero de 2011, el gobierno Alemán lanzó su estrategia de seguridad cibernética. En abril de 2011 el ministerio del interior puso en marcha el centro nacional de ciberdefensa.
AUSTRALIA	Creo el centro de operaciones cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.
CANADA	El departamento de seguridad pública implementó el centro canadiense de repuesta a incidentes cibernéticos (CCIRC), y en octubre de 2010 adoptó la estrategia canadiense de seguridad cibernética.
ESTADOS UNIDOS	Creó un centro de ciber-comando unificado que depende de la agencia de seguridad nacional (NSA, por sus siglas en inglés), DHS: National cyber security division, US-CERT: United States computer emergency readiness team y la oficina de seguridad cibernética de la casa blanca. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el centro internacional de análisis de ciber amenazas. En este mismo año es adoptada una estrategia de seguridad cibernética.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 fue adoptada una estrategia de defensa y seguridad de los sistemas de información.

Fuente: Documento CONPES 3701 [1]

V. LOS CASOS MÁS DESTACADOS DE ROBO INFORMÁTICO DE LA HISTORIA.

Si bien, a lo largo de este argumento se ha realizado un análisis detenido acerca de la importancia de salvaguardar información confidencial y de interés general o simplemente información de carácter informal. Quiero ahondar en los casos más destacados donde las barreras y rutas de protección informativa fueron vulneradas para cometer actos delictivos a gran escala.

Según el periódico "El Diario de España'' en su portal especial de tecnología "diario turing'', ninguna persona del común, especialmente los ciudadanos con altos cargos gerenciales, están exentos de ataques cibernéticos direccionados a robar información valiosa que ponga en jaque la empresa o la reputación de un individuo determinado. Por tal razón cito al director de tecnología de eyeos, José Carlos Norte, para discutir la realidad de la seguridad informática global y los casos más nombrados hasta el momento. El director de eyeos la plataforma que provee escritorios virtuales en la nube para administrar y fiscalizar archivos personales y aplicaciones para las compañías que la posean. Comentó que los ciudadanos viven en una urna de cristal, pensando que se encuentran seguros cada vez que navegan en la red, ignorando los potenciales peligros a los que se enfrentan al tener esquemas de seguridad informativa simples y vulnerables. Por tal razón, menciona que:

"La realidad es muy distinta, y cada día, miles de personas pierden dinero o intimidad a causa de ataques a sistemas informáticos de distinta naturaleza." Comentó José Carlos Norte, director de eyeos [3].

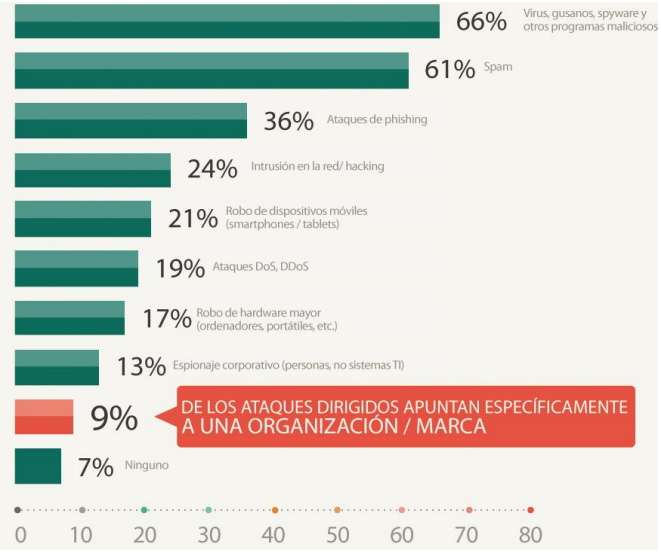

Fig. 1 Las principales amenazas informáticas en las organizaciones [10].

Partiendo de la anterior y somera introducción de las opiniones de expertos mundiales, con respecto a los ataques cibernéticos, mencionaré algunos casos donde se cometieron actividades irregulares por medio de ataques en la red.

Este caso en particular resulta interesante, debido a que en tan sólo 60 minutos los ladrones informáticos lograron traspasar casi 70 millones de dólares a varias cuentas abiertas por la organización a Viena y otros países de Europa. Ese movimiento ilegal fue consumado debido a que los implicados tenían acceso a los equipos informáticos y telefónicos del banco. Además, tenían pleno conocimiento de la operatividad del sistema interno y de las transferencias electrónicas que se realizaban periódicamente. Luego de poseer toda esa información, seleccionaron a tres de los principales inversores del banco para traspasar el dinero a las cuentas que ya tenían en operación, pero horas después, fueron descubiertos debido a la falta considerable de dinero que se había desaparecido de manera misteriosa.

Este caso aparentemente es muy común, debido a que en las empresas existen empleados con conocimientos avanzados en informática y que su único objetivo es atacar desde las entrañas institucionales y beneficiarse monetariamente o simplemente saciar su curiosidad con información valiosa y de primera mano.

Por su parte, también las instituciones gubernamentales han sufrido ataques inminentes a los núcleos informacionales de carácter confidencial sin importar si son del primer mundo o no. Este caso involucra a agencias gubernamentales, militares y empresas estadounidenses que en el año de 1998, sufrieron un ataque cibernético que develó información calificada e intransferible, luego de que varios hackers alemanes decidieran escudriñar en sus principales cuentas.

Como resultado del ataque, se expusieron planes confidenciales adelantados por estas organizaciones y que estaban direccionados a la creación de armamento nuclear con fines que aún no se han determinado.

Según la página de información de delitos cibernéticos: http://www.delitosinformaticos.info/ la compañía experta en seguridad informática, recovery labs establece una serie de recomendaciones para a los usuarios con el fin de blindar y proteger los ordenadores y la información.

Por tal razón, la compañía estableció las siguientes recomendaciones que deben tener en cuenta las personas para evitar un robo repentino de información:

1) “Actualice regularmente su sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. A veces, los sistemas operativos presentan fallos que pueden ser aprovechados por delincuentes informáticos. Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus’’.

2) “Instale un Antivirus y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de Internet’’.

3) “Instale un firewall o cortafuegos con el fin de restringir accesos no autorizados de Internet’’.

4) “Es recomendable tener instalado en su equipo algún tipo de software anti-spyware, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario’’.

5) “Utilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos’’.

6) "Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de Internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:

   a) Deben empezar por https:// en lugar de http.

   b) En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página''.

"Ponga especial atención en el tratamiento de su correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. Por ello le recomendamos que:

- No abra mensajes de correo de remitentes desconocidos.

- Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc." [4].

Por su parte, y de acuerdo a los lineamientos que en este argumento se han establecido, me permito continuar exponiendo la opinión de expertos que han dedicado su tiempo entero a debatir y luchar contra los delitos informaticos. Sin embargo existe un empresario colombiano que a pesar de combatir diariamente el robo de información cibernética, afirma que en el mundo presente hay que aprender a convivir con este tipo de actuaciones indecorosas, mientras se tenga claro que es un deber la protección para estas acciones.

En su columna personal en la revista dinero, Gerardo Aristizabal, Gerente General de mi.com.co comentó.

"En la actualidad, donde parece no existir la seguridad en internet, los audaces empresarios, y los internautas en general marcarán la diferencia en la medida que aprendan a manejar el ámbito privado y el público, a administrar técnicamente sus espacios en internet y a comportarse responsablemente tal como lo hacen en su vida normal. La seguridad en Internet, más que un derecho para los usuarios, hoy se ha convertido en un deber de los mismos. ¡A cuidarnos se ha dicho!" [5].

La opinión del gerente de mi.com.co, es muy valiosa, partiendo del hecho inherente de ver la seguridad informática como un deber ciudadano. Este planteamiento resulta interesante y preocupante a la vez, teniendo en cuenta, que el postulado nace como una necesidad de proteger la información empresarial, lo que indica que en la actualidad el número de hackers ha aumentado de manera dinámica y descomunal.

Si bien estas premisas resultan desalentadoras en un primer plano, la idea de establecer como un deber ciudadano la protección de los documentos electrónicos abren la puerta a un nuevo paradigma entorno a la responsabilidad de respetar lo privado y lo público en el entorno digital. Es decir, establecer un esquema democrático direccionado a proteger información personal de una persona común o establecer esquemas de seguridad más drásticos para las empresas e instituciones públicas.

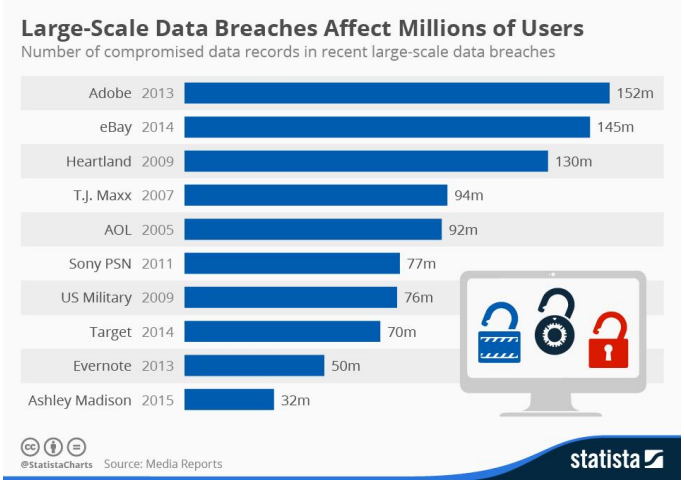

Fig. 2 Los 10 mayores ciber-ataques a las compañías tecnológicas [9].

Esto es válido recalcarlo debido al caso que se presentó en Colombia con la corporación autónoma regional de Boyacá, CORPOBOYACÁ, cuando en el año 2007 sufrió un ataque cibernético de gran escala, dejando como resultado el robo de más de mil millones de pesos.

Los hackers realizaron el ataque durante semana santa con el fin de trasladar el dinero robado a más de 18 cuentas en la ciudad de Barranquilla y Valledupar, lo cual prendió las alarmas luego de que los funcionarios del banco identificaran movimientos extraños en las cuentas bancarias de Corpoboyacá, dando aviso inmediato al Tesorero de la entidad y al Director de la Corporación.

Al final no se pudo establecer si para el traslado de esta altísima suma de dinero se utilizaron claves alternativas o si los empleados de la corporación alteraron los equipos.

Dejando la incógnita acerca del dinero proveniente del sector eléctrico y del fondo de descontaminación hídrica.

A mediados de febrero de 2012, Colombia llevó a cabo la "operación desenmascarar" una operación multinacional destinada a acabar con un anillo de delincuentes transnacionales y hacktivistas que fue lanzado en respuesta a los ataques persistentes contra las infraestructuras críticas en Chile y Colombia. La operación fue notable, ya que dependía de la colaboración entre los equipos de respuesta a incidentes y los cuerpos de seguridad de Argentina, Chile, Colombia y España. De hecho, las redadas se llevaron a cabo simultáneamente en 40 lugares y en 15 ciudades diferentes. En total, la operación desenmascarar condujo a la detención de 25 delincuentes y la captura de 250 dispositivos informáticos, junto con numerosas tarjetas de crédito robadas y dinero en efectivo [8].

VI. CONCLUSIONES

La globalización que permite el fácil acceso a la información, posibilita también las condiciones para el abuso y los ataques cibernéticos. Despertando de esta manera el interés de los gobiernos y entidades de carácter público y privado, por ejecutar acciones conducentes a proteger la información que circula en la red.

Cada país se aproxima a la ciberseguridad de manera diferente, dependiendo de su entorno económico, político y cultural imperante. Algunos países consideran principalmente la ciberseguridad como un tema de seguridad y defensa nacional. Otros lo ven como tener un mayor impacto en el desarrollo económico o la competitividad internacional. Todavía otros lo ven como un facilitador de la educación, la interacción social y la gobernabilidad centrada en el ciudadano, aunque muchos países están tratando de incorporar todas estas consideraciones en sus planes de ciberseguridad. A pesar de diversos enfoques, estudios de casos están surgiendo que ayudará a todos los países a mejorar más eficientemente sus políticas de ciberseguridad.

Muchos gobiernos se enfrentan a los rápidos avances tecnológicos con las burocracias que son lentos para adaptarse, proporcionando a hackers y las organizaciones delincuentes caminos para operar con poca preocupación de persecución o captura. Uno de los principales impedimentos para poner freno a la actividad cibernética ilícita en el año 2012 fue la falta de una legislación adecuada y las políticas de ciberseguridad.

El incremento del acceso de la población a Internet, ha potenciado simultáneamente el aumento de los ataques cibernéticos. A pesar de las medidas que ha adoptado el gobierno Colombiano por proteger la información, representadas en leyes, resoluciones y acuerdos nacionales e internacionales; “Colombia es el país de Latinoamérica que más genera ataques informáticos, con más del 20 por ciento, seguida por Argentina, Perú, México y Chile. Y un buen porcentaje de estos afectan a las empresas” [2].

La llegada de las redes sociales y las nuevas tecnologías electrónicas prometen cambiar a un ritmo increíble. Las nuevas tecnologías electrónicas y formas de usarlas pueden proporcionar oportunidades y peligro, a veces ambas cosas al mismo tiempo. El ciberespacio ha ofrecido vías directas para la creación rápida de una sociedad basada en el conocimiento. Los cibercriminales y terrorismo cibernético se empeñan en el secuestro de estos enormes beneficios para las sociedades. La creación de defensa cibernética y vanguardia de estas mentes criminales parece ser la única opción que queda por controlar y asegurar la autopista de la información.

REFERENCIAS

[1] Consejo nacional de politica económica y social, (2011, Jul). Lineamientos de política para ciberseguridad y ciberdefensa. Documento CONPES 3701 [online]. Disponible: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[2] Diario (2014, Oct). Colombia, principal fuente de ciberataques en Latinoamérica. *Diario portafolio* [online]. Disponible: http://www.portafolio.co/negocios/ataques-ciberneticos-colombia.

[3] N. Elias, (2013, May). España, Grandes robos informáticos de la historia. *Diario turing* [online]. Disponible: http://www.eldiario.es/z/Grandes-robos-informaticos-historia_0_132986921.html.

[4] Diario (2015, Sept). España, Consejos sobre seguridad Informatica. *Recovery labs* [online]. Disponible en: http://www.delitosinformaticos.info/consejos/sobre_seguridad_informatica.html.

[5] A. Gerardo, (2015, Mar). Colombia, Seguridad en Internet: más que un derecho, un deber. *Revista Dinero* [online]. Disponible en: http://www.dinero.com/opinion/articulo/la-importancia-seguridad-internet/206847.

[6] Diario (2007, Abr). Colombia, Hackers' desfalcaron $1.700 millones a Corpoboyacá durante Semana Santa. *Diario el tiempo* [online]. Disponible: http://www.eltiempo.com/archivo/documento/CMS-3508058.

[7] Symantec, (2011, Feb). Reporte sobre seguridad empresarial. [online]. Disponible: http://www.symantec.com/content/es/mx/enterprise/images/theme/enterprise-security/State-of-Security-Survey-Report-LAM-SPA.pdf.

[8] Interpol. (2012, Feb). Los hackers presuntamente vinculados al grupo 'Anonymous' en la mira de la operación global de apoyo de INTERPOL. [online]. Disponible: http://www.interpol.int/News-and-media/News/2012/PR014.

[9] R. Samuel. (2015, Agos). Los 10 mayores ciber-ataques a las compañías tecnológicas de la historia. [online]. Disponible: http://ecommerce-news.es/internacional/los-10-mayores-ciber-ataques-a-las-companias-tecnologicas-de-la-historia-infografia-30013.html

[10] M. Serge. (2013, Dic). Las amenazas más importantes de 2013. [online]. Disponible: https://blog.kaspersky.es/las-amenazas-mas-importantes-de-2013/2008/

Autor

Pedro Antonio Fula Perilla. Ingeniero de sistemas de la universidad Piloto de Colombia, estudiante de la especialización seguridad informática universidad Piloto de Colombia.